DIEZ CONSEJOS BÁSICOS SOBRE CIBERSEGURIDAD

La Rioja

1. No compartir información confidencial

Jamás compartas con nadie tu información personal. Por ejemplo, nunca facilites los datos bancarios o de la Seguridad Social o las contraseñas y nombres de usuarios a través de correos electrónicos, llamadas telefónicas o mensajes de texto, especialmente si no eres capaz de identificar con seguridad a tu interlocutor.

2. Evitar enlaces desconocidos

Es muy peligroso hacer clic en enlaces o archivos de remitentes desconocidos. Cada vez es más frecuente que contengan o dirijan a contenidos maliciosos diseñados para infectar tanto ordenadores como otros dispositivos. Su efecto puede ser devastador.

3. Usar contraseñas fuertes

Todas tus cuentas, profesionales y personales, incluso las de las redes sociales deben ser protegidas con contraseñas seguras para evitar la suplantación de identidad. Un gestor de contraseñas será de gran ayuda para evitar la repetición y reutilización continua de una clave, porque sirve para guardar y recordarlas de forma segura. Además, para el acceso a los servicios importantes, tanto en tu trabajo como en tu vida personal, el uso de un segundo factor de autenticación disminuirá las posibilidades de que suplanten tu identidad.

4. Identificar y detectar fraudes

Debes saber identificar llamadas, correos electrónicos y mensajes fraudulentos. Deberías conocer cómo son los distintos formatos de ciberestafas que intentan obtener información confidencial y acceso a tu información y hasta a tu dinero. Unos sencillos consejos pasan por revisar cuidadosamente la dirección de correo electrónico o número de teléfono, evaluar el tono y la urgencia del mensaje que incitan a actuar sin pensar, analizar los enlaces y archivos adjuntos, verifica la legitimidad del remitente incluso contactando con el remitente, desconfía de solicitudes de información personal o financiera.

5. Desconfiar de ofertas irreales

Si un anuncio te asegura que pinchando en un enlace ganarás 2000 euros o que puedes alquilar un apartamento en la playa en agosto por 500 euros la quincena, parece evidente que es una estafa digital. Aun así, seguimos creyendo en esos mensajes. Conviene analizar esos mensajes con anuncios y ofertas extremadamente atractivas con un mínimo rigor y escepticismo porque son un anzuelo para incautos. Recuerda que no es oro todo lo que reluce.

6. Actualizaciones y antivirus

Es fundamental mantener el software de tus dispositivos actualizados para corregir las vulnerabilidades que se van descubriendo. Y tienes que entender que el dispositivo ya no es solo el PC, también lo es la tableta, el móvil, la TV inteligente y hasta la aspiradora, el robot de cocina o el frigorífico. Todo lleva software que es vulnerable y está conectado a la red. Debes disponer de una protección adecuada, y el clásico antivirus es lo mínimo con lo que debes contar.

7. Evitar Wi-Fi públicas

Las redes Wi-Fi públicas son inseguras porque son administradas por desconocidos en los que no podemos depositar la confianza y porque, con frecuencia, suplantan el nombre de una red legítima para hacernos caer en un engaño. Evita la conexión a redes públicas y más cuando estas son abiertas (sin acceso con contraseña). Cuando te conectas, puedes permitir el acceso no autorizado a tus datos confidenciales por parte del administrador de esa red o de otros equipos conectados a la misma.

8. Copias de seguridad

Si dispones de información importante o sensible, cuya destrucción pueda causar un perjuicio a ti mismo o a la organización, asegúrate de que esa información dispone de una copia de seguridad que puedas recuperar en caso de incidente. Asume que es posible que no pueda recuperarse la totalidad de la información, aunque recuperar una parte siempre será mejor que no recuperar nada.

9. Comunicación y respuesta

También debes asumir que antes o después ocurrirá un incidente. Cuando esto ocurra, lo único que podemos hacer es tratar de recuperarnos de ese incidente lo antes posible. Para que esta recuperación sea lo más rápida y completa posible es imprescindible que comuniques cualquier tipo de anomalía o sospecha que puedas detectar. El Centro de Atención a Usuarios está disponible las 24 h del día todos los días de la semana.

10. Fomentar la educación continua

Mantente informado sobre ciberseguridad en fuentes fiables. No todas lo son y las falsas noticias que se mueven en redes sociales son un ejemplo claro. La Oficina de Seguridad del Internauta (OSI) de INCIBE puede servirte para estar al tanto de las últimas amenazas y técnicas de estafa en línea.

Gobierno de La Rioja.